Minnesota Trucking Association Model Incident Response Plan

Overview: This model cybersecurity incident response plan was developed in cooperation with MTA member fleets and best industry practices identified by trucking industry information technology professionals.

It is the direct outgrowth of a tabletop exercise in 2022 funded by a grant from the United States Department of Homeland Security and conducted by the Norwich University Applied Research Institute (NUARI).

This model is designed to serve as a guide to jumpstart your own plan development process. Users are advised to customize this to meet their own fleet operations AND to utilize legal and technical expertise in finalizing this plan.

For more information: www.mntruck.org or mta@mntruck.org

Insert Company Name
Cybersecurity Incident Response Plan (CIRP)

Contents

Insert Company Name
Cybersecurity Incident Response Plan (CIRP)

Plan Scope

- *Enforce the approved Cybersecurity Incident Response Policy*
- *Ensure consistent and appropriate handling of security incidents*
- *Reduce risk, expense, and down time resulting from a security incident*

This plan exists to ensure that security incidents are handled consistently and appropriately. The plan is designed to reduce risk, cost, and down time due to a security incident or catastrophic anomaly. Failure to adhere to this plan may result in compounding or exacerbation of incidents, legal liability, or other damage to the reputation or finances of **Insert company name**.

This plan does not encompass operational IT incidents (outages, bugs, etc.) that have no impact upon confidentiality or integrity or regulated information. Operational IT incidents are handled by the IT team.

The following priorities serve as a starting point for defining our organization's response:

- Protect customer information and assure organizational data integrity
- Maintain the organization's reputation and control external communication
- Prevent damage to systems
- Minimize disruption of computing resources

Authority

- *Director of IT or delegate*
    - *Communicate incidents to Executives, as necessary*
- *Director of Safety*
    - *Report incidents to legal counsel*
- *Senior Systems Engineer*
    - *Coordinate and train the Incident Response Team*
    - *Document and report incidents*
    - *Properly execute the incident response procedures*
    - *Communicate incidents to selected management*

The Director of IT is authorized to declare incident categories. The Senior Systems Engineer is responsible for coordinating and training the Incident Response Team related to Incident Response responsibilities. The Senior Systems Engineer is responsible for documenting and reporting incidents as well as overseeing the proper execution of the incident response procedures. Reporting incidents to the CEO and President is the responsibility of the Director of IT or delegate.

Communication Guidelines

- *Communications should be kept strictly on a need-to-know basis*
- *Communications should be fact-based to avoid misrepresentation of details*
- *Legal counsel should be included in all communications, written and verbal*
- *Verbal communication is preferred*

All information security incident response communications and information should be treated as restricted information and kept strictly on a need-to-know basis. This is critical to ensure protection against unauthorized disclosure and risk of litigation. In addition, all communication, written or verbal, should be strictly fact-based and not assumptions, to avoid misrepresentation of incident details.

- IT operational incident response processes will be followed, typically using the phone or in person as the primary form of ongoing communication and information exchange
- For communications occurring outside of the IT operational incident response team, verbal communication is the preferred method. If e-mail communication is initiated, and **Insert Company Name** Legal determines a need for attorney-client privilege, they will appropriately initiate the privilege with the required labeling on all communications

Roles and Contact Information

Incident Leader- Senior Systems Engineer

1. *Provide direction to the entire Information Security Response Team (ISRT)*

This role is pivotal for fast and efficient initiation of the Incident Response Process. The individual that is identified in this role should be familiar with this process. Identification of individuals willing and capable of performing this role should be done immediately upon review of this document. Chosen individuals should review the master copy of this plan on a quarterly basis and make note of any revisions or process changes.

Incident Coordinator- Director of IT

2. *Track all events throughout the entire incident handling process*

These individuals will be responsible for contacting and recruiting the required personnel to effectively reduce exposure and hail a return to normal operations. They will also be responsible for managing timeline and tracking what activities each member is currently undertaking.

Many incidents require several days to resolve. The Incident Coordinator will be responsible for working with staff management to schedule shifts to ensure that staffs are provided adequate rest to properly perform job duties. To help avoid costly mistakes, the Incident Coordinator may appoint Sub-Coordinators to relieve the Incident Coordinator of overbearing tasks, or to provide for a more granular monitoring of tasks and units of work.

Internal Communications

3. *Communicate a consistent message to the internally impacted organizations and business units*

This person does not communicate with external customers or the media; those types of communications will come through a predefined point of contact within each operating company.

Internal Contacts

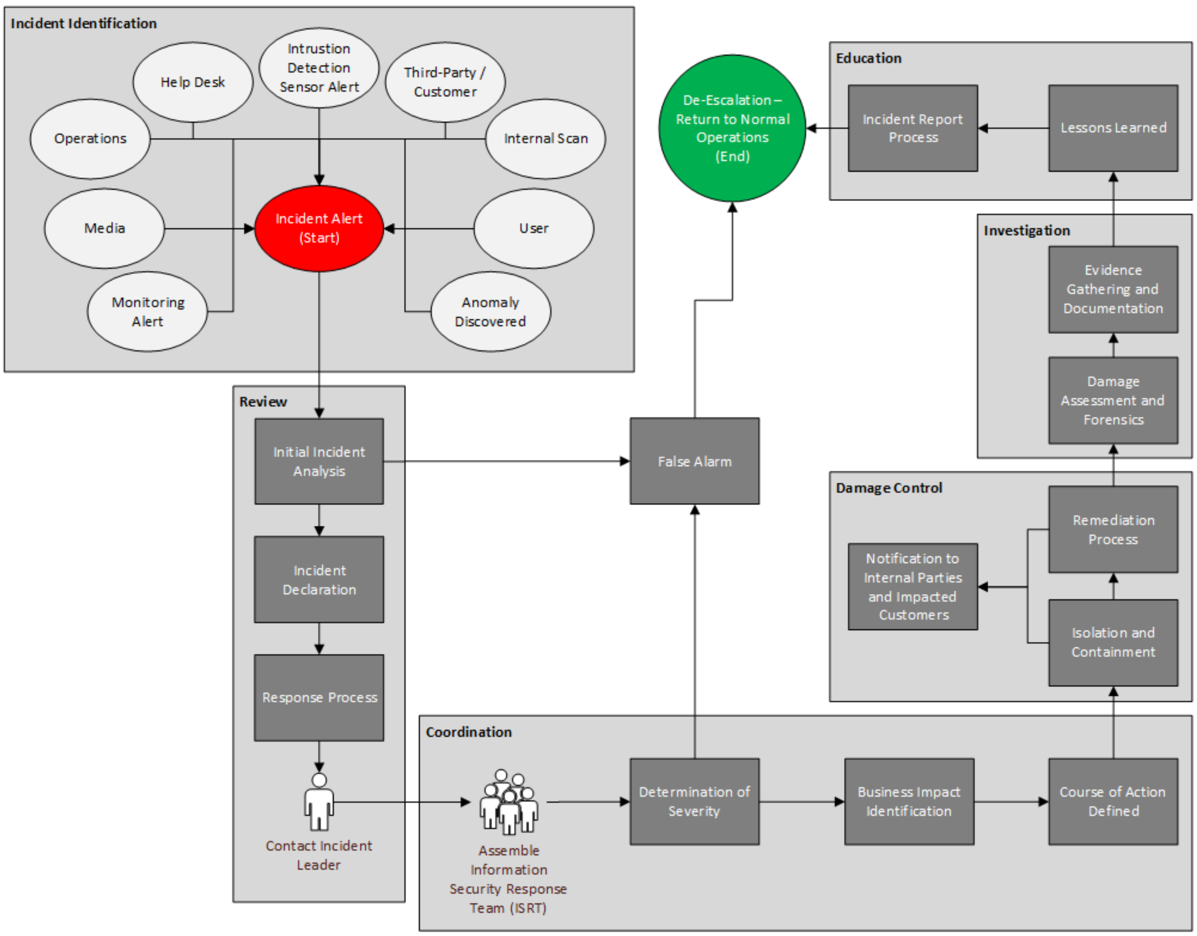
Information Security Response Team (ISRT)			
Function	***Name***	***Phone***	***Email***
Internal Incident Leadership			
Incident Leader			
Incident Coordinator			
Internal Communications			
Legal (External)			
Primary			
Backup			
Senior Management			
Primary			
Backup			
Backup			
Backup			
Backup			
Public Relations			
Primary			
Backup			
Human Resources			
Primary			
Backup			

External Contacts

External Security Response Team			
Function	***Name***	***Phone***	***Email***
Cybersecurity Consulting & Forensics Analysis			
Phone system			
Microsoft Vendor / Server Hardware			
Computer Hardware / Misc IT Software / Veeam / VMWare / Nimble / HP Servers			
Consolidated Internet and Phone Service			
Tablet Support			
FBI Minneapolis			
CyberSecurity Consultant			
Insurance			

Incident Response Process Flow

The following phases outline the process for executing the Cybersecurity Incident Response Process. Some activities may be performed concurrently. Some specific incident response examples are provided in Appendix F below.



Summary of Activities

1. *Declare it an Incident (see page 16 for classification).*
2. *(Commander/Lead) While isolation starts, contact Incident Response vendor/partner (FR Secure).*
3. *(Coordinator) – begin impact analysis and isolation.*
4. *Impact – identified which systems (servers and workstations) impacted.*
5. *Isolation/Containment – starting with servers, ensure offline to the extent needed.*
    a. *There would be a parallel separate ‘ground crew’ for desktop isolation.*
    b. *Would also do crowd control (keep end users away from server recovery team)*
6. *Restoration – restore in priority order.*
7. *(Communicator) In parallel communication to key stakeholders (All email, senior team, etc.).*
8. *Enterprise password reset (may need to do multiple time due to domain controllers [golden ticket or cobalt strike involved] depending on situation).*
9. *External vendor password reset (customer/vendor portals, etc.).*
10. *Complete internal/external communication.*
11. *Digital forensics to determine damage (exfiltration of data, etc.).*
12. *Begin hardening and fortification process.*

Incident Identification

Incident Alert

13. *Initial intake of the details of a potential incident*

Incidents alerts can be generated from many sources. Some examples include monitoring alerts, the media, operations, help desk, intrusion detection sensor alerts, third-parties, customers, internal scans, users, or other anomalies. All incident alerts should be taken seriously and require some degree of analysis.

Roles and Responsibilities: The team member assigned to start the process should receive the incident notification and initiate the remainder of the process as described below.

Review Phase

Initial Incident Analysis

14. *Determine the validity of the incident*
15. *Determine the overall approach to handling the incident*

This process involves a high-level identification of the event and a determination of the validity of the incident. If the individual that received the initial notification is uncertain of the validity, they are required to escalate to the next step in the process. **Any uncertainty of the validity requires escalation to the next level of management.**

Many incident notifications can generate false alarms. As the incident handling capabilities mature the number of false alarms should decrease. Regardless, each alert will be treated as real and requires a staff member to perform an Initial Incident Analysis.

At the Director of IT and Senior Systems Engineers discretion, based on the type of incident, the overall approach to an incident may be as follows:

1. Overview – What are the goals and objectives in handling the incident?
2. Evaluation and Classification –
    a. How serious is the incident?
    b. Is there a possibility that we will need to notify our customers?
    c. Is this a multi-site incident?
    d. Are many computers at your site affected by this incident?
    e. Is sensitive information involved?
    f. What is the entry point of the incident (network, phone line, local terminal, etc.)?

   g. Is the media involved?
   h. What is the potential damage of the incident?
   i. What is the estimated time to close out the incident?
   j. What resources could be required to handle the incident?
   k. What is the initial Severity Rating?
3. Notification - Who should be notified about the incident?
4. Response - What should the response to the incident be?
5. Legal/Investigation - What are the legal and prosecutorial implications of the incident?
6. Documentation Logs - What records should be kept from before, during, and after the incident?

Roles and Responsibilities: A member of the ISRT will be responsible for reviewing all incidents and following the steps outlined above.

False Alarm

- *Determine that an incident a false alarm*
- *Prepare a course of action to return to normal operations*

A false alarm can occur; the owning support group working with Security will develop a course of action for these types of events when encountered.

Roles and Responsibilities: A member of the ISRT will be responsible for reviewing all incidents and correcting false alarms.

Incident Declaration

- *Determine that an incident is not a false alarm*
- *Contact Chief Process Officer*
- *Turn event ownership over to ISRT member*

Incident Declaration is the step in which a determination that the event is (potentially) real. Any uncertainty in the prior step requires escalation. Once an incident is declared the Director of IT or Chief Process Officer must be contacted. Once contacted, ownership of the event is handed over to that member of the response team. It will then be the responsibility of that ISRT member to initiate the next steps in the Response Process.

Roles and Responsibilities: Anyone that believes a security related event is or has occurred must escalate if there is uncertainty. A decision can be made by an ISRT member to de-escalate if the incident is a false alarm.

Response Process

- *Identify the required resources*
- *If CRITICAL, contact FR Secure and get Incident Response agreement in place.*
- *Escalate into the Coordination Phase*

Any member of ISRT can initiate the Response Process. After a member of the team has been notified, that person will be responsible for identifying the initial required resources. Once a potential threat has been determined, the individual will start the Coordination Phase of the Incident Response Plan and assemble the entire ISRT.

Roles and Responsibilities: The member of the ISRT has two options, the first option is that the event is a false alarm and can be de-escalated; the second option is to begin the coordination phase. **Any uncertainty must be escalated to the next phase.**

Contact Incident Leader

- *Contact Incident Leader*
- *Begin Coordination Phase*

After the Response Process has been completed, the Incident Leader will be contacted to begin the Coordination phase.

Roles and Responsibilities: The Incident Leader will assemble the ISRT to begin the Coordination phase.

Coordination Phase

Assemble Information Security Response Team (ISRT)

- *Assemble ISRT team members*
- *Initiate appropriate communications*
- *Open an Event Control Log*

Upon notification that an incident has been declared it is the duty of the Incident Leader to begin assembling team members. This process may involve initiation of conference bridge. Members of ISRT are selected based on their position, skills, experiences, and knowledge of **Insert Company Name**' infrastructure and business components. As a team, the group will determine the severity of the incident and begin identifying the impact to the business and define a course of action to handle the incident.

An ISRT member will initiate an Event Control Log. A general, pre-determined email will be initiated to provide an advisory notice to all senior leadership members and Help Desk (24x7) organizations. If deemed critical, a general email notice will be sent to all employees.

The Event Control Log will be updated on a regularly basis, and is to contain all activities, assigned tasks, setbacks, and progress. The log should attempt to identify impacted systems and business units that may be affected.

The ISRT member that is responsible for the Event Log will document the course of action to ensure that the right individuals are taking correct steps. Since incidents often occur in off-hours, this log will document individual responsibilities in case there is a need for someone to be relieved after a certain number of hours.

Roles and Responsibilities: ISRT members are required to post a 24x7 contact number to ensure availability of resources. In an instance where required ISRT members cannot be contacted and escalated resource will be assigned, and they will fulfill the required role. In addition, an assigned ISRT member is responsible for correlating and logging event into the Event Control Log. If this member believes that more much information exists than they can properly document that member should request additional support resources.

Determination of Severity

- *Verify that the incident is not a false alarm*
- *Determine initial incident severity*

Once the ISRT has assembled, the Determination of Severity will be examined. It is important that the Event Control Log capture any change in severity rating or course of action. The team will rate the severity using industry research, vendor recommendations, and by gauging the exposure based on the knowledge of our business and systems. An attempt will be made by the ISRT to figure out the extent of the potential damage and the need for additional resources.

A possibility exists that the assembled team will determine that the incident is a false alarm and will flag the event as such, which will cause a de-escalation and a return to normal operations.

The Senior Systems Engineer must review all incidents to sort between the following levels of severity:

Rating	Definition	Example
CRITICAL (Level 0)	Anything that has potential to **disrupt business on a massive scale.** Any type of **regulatory compliance that is compromised.**	A system exploit that allows a worm to propagate through the enterprise infecting servers and disrupting network functionality. Credit card information that may have been exposed to unauthorized personnel. Loss or exposed sensitive data, or personal information.
HIGH (Level 1)	**HIGH-1** Events are classified as anything that has potential to **disrupt business on a large scale.**	A system exploit that disrupts only systems in one building.
Moderate (Level 2)	**Moderate-2** Events are classified as anything that is likely to cause service **disruptions to isolated grouping of systems.**	A system exploit that does not impact many systems and would be difficult to take advantage of more than one machine.
Low (Level 3)	**Low-3** Events are classified as anything that is reported but **does not pose any real risk to the organization.**	An exploit to Windows 10, which may be in use in small pockets throughout the organization but does not represent any real risk.

Roles and Responsibilities: Each member of the core ISRT is responsible for staying current on information security tools, techniques, and information. The knowledge will aid the team and the company in fast and accurate resolution.

Business Impact Identification

- *Identify impacted systems, as well as other potentially vulnerable systems*

Based on the information that has been gathered, the ISRT will attempt to identify impacted systems and any other potential systems that may be vulnerable to the same type of vulnerability.

Roles and Responsibilities: Security, desktop and network support will provide scans of the enterprise to help detect areas where hardware or software is vulnerable. Using this information and industry research, a comprehensive business impact analysis will be generated.

Course of Action Defined

- *Put together a detailed, prioritized course of action for dealing with the event*

Once the business impact has been identified the ISRT will define a course of action. This plan includes communicating with stakeholder teams, identifying critical individuals, required tool sets, impacted systems, rating of priorities, and assignment of responsibilities.

Roles and Responsibilities: Members of the ISRT should coordinate and delegate responsibilities to cover communications, issue identification, and mitigation plans.

Damage Control Phase

Isolation and Containment

- *Determine how to isolate and contain the event to prevent its permeation*
- *Review the impact of any actions against ongoing business processes*

This process involves limiting the extent of the exposure. Assuming that isolation is possible it may be necessary to temporarily take hosts or network segments offline in order to reduce or contain the event.

In certain circumstances the ISRT will be required to make a judgment call on the severity of the attack and the impact of taking a system (or systems) offline. This step is done with caution and with the knowledge that revenue loss may occur. The ISRT may need to escalate the problem to the Emergency Management Team in order to obtain a correct level of business decision.

The ISRT may decide to take a system offline or apply an emergency (untested) patch if they believe it is in the best interest of the organization.

The team will attempt to take a phased approach, for instance if a single system is causing an enterprise-wide problem a tiered approach will be taken. An example would be:

- An attempt will be made to shut down the offending system
- If the system cannot be shut down the network port will be disabled within the switch
- An attempt will be made to have someone onsite review the system
- If the problem persists the subnet will be disabled
- If the offending system is across a WAN link, that link may be disabled to protect the rest of the enterprise
- Stop a business process if sensitive information is being improperly handled

A goal of the ISRT is to maintain a contact list for customers and the assets associated with each major business application.

Roles and Responsibilities: The ISRT is responsible for engaging the required individuals throughout the COMPANY support infrastructure to accomplish required objectives for this step. ISRT members have contact information to access all 24x7 support organizations. The 24x7 support groups are tasked with contacting their client base and provide information regarding any application outage.

Notification to Internal Parties & Impacted Customers

- *Communicate the current situation, as well as the planned remediation, to the appropriate parties*

To decrease rash decision making, the notification process occurs after a course of action has been defined in the incident flow process. The ISRT will make every attempt to get people and teams involved at the earliest possible moment once a definitive plan has been decided.

Impacted i**nternal** Crisis Teams will be given the conference bridge number to participate in discussions surrounding the incident and the summary of the business decisions.

Impacted **external** customers should be notified by business unit contact, which deals with the customer on a regular basis. Care should be taken in responses provided to external customers to alleviate overreaction, miscommunication, loss of customer confidence, or any other unwanted activity. Every effort should be made to keep external customers informed with accurate information. The decision to contact external parties should be made with great care (in a timely manner) and the business unit may consult with public relations or legal prior to contacting an external customer.

Roles and Responsibilities: Public Relations and Legal Counsel are maintained for contracted business obligations.

Further Notification guidelines can be found in Appendix C.

Remediation Process

- *Collect forensics for future analysis*
- *Restore systems to an operational status*
- *Continue to look for additional vulnerabilities*

The remediation process involves restoring systems to a satisfactory approved configuration, which could include security patches that protect the asset against the original vulnerability.

It is important that the ISRT have time to properly review the impacted system, collect forensic images if litigation or law enforcement participation becomes a necessity, and remove any backdoors or system defaults.

Roles and Responsibilities: ISRT members will work with support staff to return systems to a fully operational status in a time sensitive manner.

Investigation Phase

Damage Assessment and Forensics

- *Assess the impact from the event*
- *Review and catalog forensic data*

The damage assessment and forensics step will attempt to assess the total impact of the incident. Forensic data may be required for possible legal action, or as part of the education process in mitigating similar future events.

Any forensic data will be stored in a secure password protected location; this will ensure that no tampering occurs.

Roles and Responsibilities: ISRT forensic team members, as assigned, should take the time to review the total impact from the event, as well as properly document and protect forensic evidence for future needs.

Evidence Gathering and Documentation

- *Properly gather, document, and store the forensic information*

The incident response team should maintain records about the status of incidents, along with other pertinent information.

When an incident is a result of a computer crime, evidence can be derived from computers and then used in court against suspected individuals. Computer evidence is like any other evidence; it must be authentic, accurate, complete, convincing to juries, and in conformity with common law and legislative rules. Thus, the evidence gathered from suspected computer-related crimes must conform to the same standards as other evidence to be credible.

The Senior Systems Engineer is responsible for managing and collecting forensic evidence. The following rules will be followed:

- Ensure that no forensics evidence is damaged, destroyed or otherwise compromised by the procedures used during the investigation.
- Never work on the original evidence.
- Establish and maintain a continuing chain of custody.
- Document everything.
- Consider hiring a third party to collect evidence in a forensics-proof manner. The independence of a third party will increase credibility of evidence, and the appropriate vendor will be trained to identify, acquire, and preserve evidence in the proper manner, as well as keep a proper chain of custody.
- The Director of IT has the authority to hire and/or retain a third party to collect Forensics data so that independence is established and there is no appearance of a conflict of interest.

Roles and Responsibilities: Forensic data will be handled and safeguarded by the ISRT forensic team captain. Documented procedures for handling sensitive data will need to be developed and added to this plan.

Educational Phase

Lessons Learned

- *Establish the details surrounding the event*
- *Communicate the full extent of the damage*
- *Define improvements to prevent this type of event from happening again*

Post incident Review is a crucial part of the process. Understanding what happened and how it occurred is key to ensuring that a reoccurrence of similar events is not successful in the future. Each incident is to be viewed as a learning opportunity. The IT Security Group understands that successful attacks will occur and has built this plan to mitigate risk and to create a consistent process for dealing with incidents.

This process should occur in three phases, the first phase requires that ISRT members meet and discuss the incident to build an understanding of the details surrounding the event. This includes reviewing the Incident Report, and the Event Control Log for any relevant information.

The second phase will be a meeting with the impacted parties to discuss and understand the full extent of the damage.

A subsequent third phase meeting will be scheduled to review details around the incident to ensure that each step of the process has been followed and to decide if any improvements need to be made. Once these meetings have taken place, the Incident Report will be closed with a summary of all findings.

Determination of who will ultimately be responsible for providing the report will rely on the members of the ISRT that were involved with the incident. A copy of this report will be presented to executive management.

The following activities should occur as part of lesson learned:

- Lessons learned discussions should be held with all involved parties after a major incident, and optionally after lesser incidents, to identify gaps or weaknesses in incident response processes or technical, administrative or physical controls. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:
    - *How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?*
    - *What information was needed sooner?*
    - *Were any steps or actions taken that might have inhibited the recovery?*
    - *What would the staff and management do differently the next time a similar incident occurs?*
    - *How could information sharing with other organizations have been improved?*
    - *What corrective actions or added controls can prevent similar incidents in the future?*
    - *What precursors or indicators should be watched for in the future to detect similar incidents?*
    - *What additional controls should be implemented to improve the quality or speed of investigations?*
- All incident documentation should be finalized to enable any management reporting, metrics and monitoring and stored / retained on the appropriate location.

Roles and Responsibilities: All ISRT members, support staff, and IT management will be involved in the lessons learned section to educate and reduce the chances of a recurring event.

De-Escalation – Return to Normal Operations

Two circumstances will flag a return to normal operation. The first circumstance is that the incident was defined as a false alarm event. The second circumstance is the generation of an Incident Report from the assigned ISRT member.

Once the incident is closed, all change records should be updated to reflect all activities in the process. Calls should be placed to any teams that were involved, client management, and any affected external customer.

Roles and Responsibilities: Alerts should be documented in the change or problem ticketing systems, and a return to normal operations should occur.

APPENDIX A – Call Tree

Priority Contacts in case of incident:

1. *Insert Name*, Senior Systems engineer
    a. Mobilize team to isolate, contain, and recover.
    b. Contact appropriate technology vendors for external help.

2. *Insert Name*, Director of Safety
    a. Contact insurance company(s) as needed for claims and direction.
    b. Contact Legal firm(s) for guidance on any major event/breach matters.

3. *Insert Name*, Director of IT
    a. Contact executive team or anyone else pertinent.
    b. Included on larger decisions with large financial or brand impacts.

4. *Insert Name*, Chief Strategy Officer
    a. Handle external/PR type communication.
    b. Weigh in on and possibly send internal email communication.

5. *Insert Name*, Director of Logistics
    a. Contact Logistics personnel
    b. Contact customers with assistance from CSO (see number 4)

6. *Insert Name*, Chief Operation Officer
    a. Contact direct reports as appropriate

7. Operational Management Team
    a. Contact drivers and customers as appropriate with assistance from CSO

APPENDIX B – Incident Classification Guidelines

The incident type and impact will determine the level of response needed by **Insert Company Name**. The Information Security Officer will work with departments to determine the appropriate response for each confirmed incident. The general steps required for incident categorization and classification are:

1. Categorize the incident based on type of incident, security objective, and impact.
2. Classify the incident as a local or enterprise incident.
3. Prioritize handling of the incident based on the **Insert Company Name** Incident Response Classification Matrix
4. Activate CIRP if necessary
5. Report the incident to the appropriate internal personnel and external organizations

COMMON CATEGORIES OF CYBER INCIDENTS

Incident Type	Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a COMPANY network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Employees are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
Improper or Inappropriate Usage	When a person violates acceptable computing policies.
Suspected PII Breach	If an incident involves personally identifiable information (PII) a breach is reportable by being merely Suspected. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.)
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred as a result of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) Use, where the cause or extent is not known.

IMPACT DEFINITIONS

Security Objective	Potential Impact		
	Low	**Medium**	**High**
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity: Guards against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

APPENDIX C – Notifications

Notifications must be timely, clear and conspicuous and delivered in a manner that will ensure the correct person(s) is likely to receive it. The notification may be by phone or mail or for customers who conduct transactions electronically, electronic notice may be given.

External communications to customers, law enforcement and/or the media must be reviewed by the Chief Strategy Officer and presented to Management for approval prior to releasing it to the press.

Customer Notification:

1. Assess the nature and scope of the incident and identify what customer information systems and types of customer information have been accessed or misused.
2. Notify your primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
3. File a timely response, and in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, promptly notify appropriate law enforcement authorities.
4. Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information; and
5. Notify customers when warranted in a manner designed to ensure that a customer can reasonably be expected to receive it.

If customers need to be notified, the Director of Safety will determine if legal counsel must be involved. Notification should include the date of the breach and the types of information that was breached. Notification should be reviewed by the PR / Marketing member of the prior to delivery. The Board of Advisors must be notified in the event of a Customer Notifications.

Board of Advisors:

The Board of Advisors will be informed, in real time, of any incidents which require notification of customers, law enforcement, or other government agencies. The Board of Advisors will also receive a summary of incidents annually in the Annual Information Security Report to the Board.

Customer Financial Notification:

1. Describe the incident
2. Indicate the customer's information that was accessed
3. Provide a telephone number for the customer to call for additional information
4. Remind the customer to be alert for the next 12-24 months and promptly report any incidents of suspected identity theft.
5. Inform the customer XXX BANK will assist in correcting and updating any information in any consumer report, as required by the FCRA.
6. Recommend that the customer notify each nationwide credit reporting agency to place a fraud alert in the customers consumer report.
7. Recommend the customer periodically obtain credit reports
8. Inform the customer of the right to obtain a free credit report if the customer has reason to believe their report may contain fraudulent information.
9. Inform the customer of the FTC's online guidance regarding prevention of identity theft.

The notice may:

10. Provide a toll-free telephone number for customer contact.
11. Offer to assist the customer in notifying credit reporting agencies

Inform the customer of subscription services that will notify the customer anytime there is a request for their credit report or offer to subscribe the customer to this service free of charge, for a period of time.

Law Enforcement Notification:

Law Enforcement will be notified if the incident warrants a criminal investigation. This includes, but is not limited to, theft of computer equipment or software, destruction of or tampering with government equipment, illegal Internet activity, electronic mail that poses a threat to customers or staff and falsifying or stealing information contained in company systems. Investigative procedures will be followed to determine if criminal activity occurred. Pending preliminary investigation results, the Director of Safety will work with law enforcement to meet further reporting requirements. Management will be kept informed of the progress of the investigation as changes in the status of the investigation occur.

If law enforcement must be notified and an investigation initiated, a Suspicious Activity Report (SAR) must be filed with the Financial Crimes Enforcement Network (FinCEN). It is up to the Director of Safety and Chief Process Ofiicer's discretion as to whether incidents warrant the involvement of Law Enforcement and/or submission of a SAR to FinCEN. Note however, that Bank Secrecy Act regulations require every financial institution to file a report of any suspicious transaction relevant to a possible violation of law or regulation.

Public:

One of the most important issues to consider is when, who, and how much to release to the general public through the media. There are many issues to consider when deciding this issue. The public relations office is trained in the type and wording of information released and will help to assure that image is protected during and after the incident (if possible). Involving the public relations office substantially reduces reputational risk. A public relations officer has the advantage to communicate candidly with the public and then act as a buffer to the media so that control over the incident is maintained.

If a public relations officer is not available, the information released to the media must be carefully considered. If the information is sensitive, it may be advantageous to provide only minimal or overview information to the media. It is quite possible that the perpetrator of the incident will quickly review any information provided to the media.

While it is difficult to determine in advance what level of detail to provide to the media, some guidelines to keep in mind:

- Keep the technical level of detail low. Detailed information about the incident may provide enough information for copycat events or even damage the company's ability to prosecute once the event is over.
- Keep speculation out of media statements. Speculation of whom is causing the incident or the motives are very likely to be in error and may cause an inflamed view of the incident.
- When necessary, the Director of Safety, Chief Process Officer, Director oif IY and Senior Systems Engineer will work with law enforcement professionals and/or third-party forensics experts to assure that evidence is protected. If prosecution is involved, assure that the evidence collected is not divulged to the media.
- Try not to be forced into a media interview before you are prepared. The popular media is famous for the “2 a.m.” interview, where the hope is to catch the interviewee off guard and obtain information otherwise not available.
- Do not allow the media attention to detract from the handling of the event. Always remember that the successful closure of an incident is of primary importance.

When the incident is closed, the Chief Process Officer or Director of IT (or a designated party) will report the following:

- a description of the incident.
- the response processes.
- the notification processes.
- the actions taken to prevent further breaches of security.

Furthermore, a Suspicious Activity Report must be filed with the appropriate authorities.

APPENDIX D – Standard Bridge Conference Lines:

In order to standardize the channels into the Incident Management function, the following conference bridges are to be used. Incident Managers identify the appropriate bridge to be used through their initial communication at the time of the incident.

Conference Bridge

Tactical Room: (Command Center)

- Ad hoc Teams Room – Communicator will open this

Strategic Room

- Text Message: to notify team
- Ad hoc Teams Room – Communicator will open this

APPENDIX E – External Contacts

FBI FIELD OFFICE

Call the national infrastructure protection and computer intrusion squad at the local field office.

Minneapolis
1501 Freeway Boulevard
Brooklyn Center, MN 55430
https://www.fbi.gov/contact-us/field-offices/minneapolis
(763) 569-8000

Internet Crime Complaint Center (IC3)

https://www.ic3.gov/default.aspx

CYBER INVESTIGATIONS BRANCH OF THE U.S. SECRET SERVICE HEADQUARTERS

950 H Street, NW
Washington, DC 20223
phone: (202) 406-5850
fax: (202) 406-5031
website & reporting:
https://www.secretservice.gov/investigation/cyber
https://www.secretservice.gov/contact/field-offices

FEDERAL AGENCIES, WASHINGTON

FBI/National Infrastructure Protection Center (NIPC)
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001
phone: (202) 323-3205; 888-585-9078
fax: (202) 323-2079
e-mail: nipc.watch@fbi.gov
website: http://www.nipc.gov
reporting: http://www.nipc.gov/incident/cirr.htm

ELECTRONIC CRIMES BRANCH OF THE U.S. SECRET SERVICE HEADQUARTERS

950 H Street, NW
Washington, DC 20223
phone: (202) 406-5850
fax: (202) 406-5031
website & reporting: http://www.treas.gov/usss

STATE & LOCAL AGENCIES

State Attorney General's Office The website for the National Attorney Generals' Association provides a list
with contact information by state. http://www.naag.org/issues/20010724-cc_list.cfm

Local Police: The CrisNet website offers a list of local law enforcement agencies organized by state.
http://www.crisnet.com/locallaw/locallaw.html

OTHER REPORTING BODIES & RESOURCES FOR CYBERTHREAT SUPPORT

Most of the following organizations not only serve as coordination points for reporting incidents, but they also offer lots of useful information for network security and incident response.

National Infrastructure Protection Center (NIPC)
Focal point for threat assessment, warning, investigation and response for threats or attacks against United States critical infrastructures.
http://www.nipc.gov

InfraGard
Public/private information-sharing effort led by the FBI and the NIPC. Local chapters across the United States.
http://www.infragard.net

Electronic Crimes Task Force
Public/private info-sharing effort led by the U.S. Secret Service. Regional task forces located across the United States, and a great place to develop computer-crime law-enforcement contacts.
http://www.ectaskforce.org/Regional_Locations.htm

Information Sharing & Analysis Centers (ISACs)
Industry specific information sharing for critical infrastructure sectors. For general information on the ISACs, see
https://www.it-isac.org/isacinfowhtppr.php
Electric . . . . http://www.nerc.com
Financial Services . . . http://www.fsisac.com
IT . . . . http://www.it-isac.org
Oil & Gas . . . . http://www.energyisac.com
Telecom . . . . http://www.ncs.gov & www.ncs.gov/Image-Files/ISAC_Fact.pdf
U.S Govt. . . . . http://www.fedcirc.gov
Water . . . . http://www.amwa.net/isac/

Payment Card Brands:

The payment card brands have specific requirements for reporting and responding to suspected or confirmed breaches of payment card data. As a merchant business your primary contact if an incident occurs should always be your acquirer. It is worthwhile referring to the links below to familiarize yourself with the detail of the card brands' recommendations around how to respond to Account Data Compromises and what their specific requirements are.

MasterCard:
https://www.mastercard.us/content/dam/mccom/en-us/documents/account-data-compromise-manual.pdf

Visa Global:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

American Express:
https://www209.americanexpress.com/merchant/services/en_US/data-security (includes links to all information for all territories)

Discover Card:
http://www.discovernetwork.com/merchants/fraud-protection/index.html

APPENDIX F – Specific Incident Responses

This Cybersecurity Incident Response Plan provides the generic steps that must be followed when dealing with a security incident.

Some specific incident types requiring additional response actions are provided below.

Malware (or Malicious Code)

An Advanced Persistent Threat (APT) such as a worm, virus, Trojan horse, ransomware or other code-based malicious entity that infects a host.

Initial Analysis

i. On call/point person review ticket/validate (SLA – 1 hour) = event
ii. Review ticket with team = event until group determines incident
iii. Review endpoint logs
iv. Pinpoint location
v. Run AV scans on machine
vi. Discuss incident with reporter or end user

Post declared Incident

vii. IT disconnect devices identified with malware from the network immediately.
viii. Help Desk scans endpoint or installs additional tools
ix. Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device. This will help you to understand how to remove it from the device.
x. Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.
xi. If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware.
xii. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

Tampering of payment terminals, chip & PIN/signature devices or card readers detected, Card-skimming devices found, or devices substituted

i. Stop using the substituted/tampered devices
ii. Report the substitution/tampering to your device provider and your acquirer
iii. Follow your device provider or acquirer's advice to ensure the security of all future card payments, e.g. inspect and confirm the integrity of your remaining devices, deploy replacement devices, etc.
iv. Follow your device provider or acquirer's guidance to investigate the incident e.g. send the substitute/tampered devices to them, allow on-site investigations, etc.

Unauthorized Wireless Access Points

If unauthorized wireless access points are detected, or reported by staff, these must be recorded as a security incident.

i. SIRT will investigate to identify the location of the unauthorized wireless access point/device.
ii. The SIRT will investigate as to if the unauthorized wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
iii. All other unauthorized wireless access points/devices must be located, shutdown and removed.

Loss of Equipment

i. The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the SIRT and local law enforcement. This includes losses/thefts outside of business hours and at weekends.
ii. If the device that is lost or stolen contained sensitive or payment card data, and the device is not encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen, including any potentially exposed payment card numbers.
iii. Where possible, SIRT will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

Non-Compliance with your Security Policy

This covers incidents resulting from deliberate or accidental actions that are in breach of your security policy and which put sensitive or payment card data at risk. This includes any systems or data misuse, unauthorized exposure of data to external parties, unauthorized changes to systems or data.

i. SIRT will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
ii. SIRT and/or line managers will notify Human Resources of the incident.
iii. SIRT will liaise with Human Resources and line managers to determine whether disciplinary action is needed.
iv. SIRT will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example re-training of staff.

Other Types of Incidents

Examples of information security incidents may include, but are not limited to:

- **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- **Unauthorized Access/System Hijacking:** A person gains logical or physical access without permission to a network, system, application, data, or other resource
- **Unplanned Downtime:** The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime
- **Multiple Component:** A single incident that encompasses two or more incidents (e.g., a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to other hosts)

- Other examples of observable information security incidents may include, but are not limited to:
    - Use of another person's individual password and/or account to log into a system
    - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment)
    - Leaving workstations unattended while actively signed on
    - Installation or presence of unauthorized software
    - Falsification of information
    - Theft of equipment or software
    - Destruction of tampering with equipment or software
    - Posting of PHI on the Internet from a web portal
    - Discarding of PC hard drives, CDs or other devices including PHI without following approved destruction/disposal guidelines
    - Terminated workforce member accessing applications, systems, or network
    - Compromise of Confidential or Personally Identifiable Information
    - Compromise of Card Holder Data (PCI DSS)
    - Excessive Port Scans
    - Firewall Breach
    - Virus Outbreak
    - Compromised Systems or Webpages
    - Unauthorized access to a computer
    - Loss of information confidentiality, integrity or availability
    - A denial of resources
    - Misuse or abuse of systems or information
    - Physical or operational damage to systems
    - Presence of malicious processes and applications
    - Creation of an unauthorized account for a computer or application
    - Unusual or suspicious network activity
    - Unusually slow performance

APPENDIX G – Examples of Reportable Incidents

The following are examples of reportable incidents.

1. Using another person's individual password and/or account information.
2. Failure to protect passwords and/or access codes (e.g. sharing individual codes; taping to equipment to avoid memorizing).
3. Accessing customer records for other than a "need to know" reason.
4. Asking unauthorized personnel to access your personal record/data.
5. Unauthorized personnel accessing a co-worker's record in response to their request.
6. Leaving a workstation signed on/unattended; failure to log off.
7. Unscheduled system downtime.
8. Unauthorized use of external computer connections (e.g. modems).
9. Installation of unauthorized software (screensavers, games, etc.).
10. Indication of computer virus.
11. Illegal reproduction of customer data.
12. Inappropriate disposal of customer data.
13. Falsifying data (customer, financial, employee, mission critical, etc.).
14. Disclosing customer information with unauthorized personnel; failure to safeguard confidential data.
15. Theft of computer equipment or software.
16. Inappropriate use of software, such as illegal copying of licensed computer software, intentional introduction of computer viruses, etc.
17. Inappropriate use of the Internet.
18. Inappropriate use of e-mail.
19. Defacing the COMPANY's website.
20. Destruction or tampering with the COMPANY equipment.
21. Negative post by a customer or non-employee on a Social Media Site.
22. Negative post by an employee on a Social Media Site.

APPENDIX H – Potential Incident Report

☐ **CHECK HERE IF DISCLOSURE INCIDENT**

Date: __________

Name: ___________________________________ Title: ________________________

Location of Incident: ____

Person(s) Involved in Incident: ____

Description of Incident: ____

____

____

____

____

____

Please attach supporting documentation.

Information Security Office Use Only — Date of Receipt: _______________

Initial Severity Level Assignment: ______________

CIRP Submission Date: ______________________

CIRP Review Summary:

____

____

____

____

Response to Incident:

____

____

____